ENHANCEMENT TO AUTHENTICATION PROTOCOL THAT USES A KEY LEASE

ABSTRACT OF THE INVENTION

A method and system for using a key lease in a secondary authentication protocol after a primary authentication protocol has been performed is described. In one embodiment, the primary authentication protocol comprises a strong, secure, computationally complex authentication protocol. Moreover, the secondary authentication protocol comprises a less complex (compared to the primary authentication protocol) and less secure (compared to the primary authentication protocol) authentication protocol which can be performed in a length of time that is shorter than a length of time required to perform the primary authentication protocol. In an embodiment, the key lease includes context information. Moreover, a new session encryption key is computed after each time a quick re-authentication is performed by executing the secondary authentication protocol using the key lease, whereas the session encryption key is used for encrypting communication traffic, providing a solution to the potential communication traffic replay threat.